



# Cybersecurity in the Digital Age: The Unseen Battle We Must Win

Representative Mike Giallombardo  
FLORIDA HOUSE OF REPRESENTATIVES

**I**n the last decade, as technology has advanced at an unprecedented rate, the rise in cyber attacks has become a significant threat that many organizations, both public and private, were unprepared for. From denying services to cyber extortion, better known as ransomware, these attacks have wreaked havoc across the globe. For the first time in history, private companies

face direct threats from foreign adversaries like China, Russia and Iran.

During my time in the legislature, I witnessed several notable cyber attacks: the attack on Tallahassee Memorial Hospital, the Colonial Pipeline incident, and more recently, the OneBlood attack on the private side. On the public side, Florida has also faced its fair share of cyber challenges,

including attacks targeting our election systems, the Department of Juvenile Justice, and the Department of Health. It is not a matter of “if” these attacks will happen but “when”.

Traditional IT staff often do not possess the same skill level as some of these sophisticated cyber attackers. In many cases, these attackers exploit vulnerabilities in systems that one would never anticipate. For instance, in 2014, Target suffered a cyber attack when hackers infiltrated through the system managing their HVAC. In another case, a casino was compromised through a fish tank thermometer connected to their network. More recent attacks have targeted cybersecurity software itself, corrupting the entire network when a malicious update is pushed.

So, the pressing question is: How do we defeat this growing threat? While there are countless solutions being sold along with various ideas being floated, I believe there are multiple steps we have to take. To start, we have to defend our networks and infrastructure by encouraging entities to meet the rigorous cybersecurity standards that have already been established and are continuously updated. Standards such as NIST, SOC 2, HITRUST, or ISO 27001 provide robust frameworks for cybersecurity, but most entities are not required to adhere to any of these standards.

In today’s digital age, where virtually everything is stored electronically, we need to incentivize both companies and government bodies to comply. One way to achieve this is by limiting negligence litigation for those who substantially comply. What many do not realize is that after a major

cyber attack, especially in Florida, lawsuits often follow. For instance, after a hospital pays a ransom to unlock their systems, they may face additional financial burdens from lawsuits. I recall a hospital paying \$8 million in ransom and another \$8 million in a lawsuit. A class action suit might offer those affected \$50 and a lifetime of identity theft protection while the attorneys walk away with millions. By providing liability protection to entities that substantially comply with cybersecurity standards—standards that even some state agencies do not fully adhere to—we can strengthen our cyber defenses and provide an incentive for all entities to improve their cyber defenses.

Some may question why we should allow substantial compliance rather than full compliance. The answer is straightforward: achieving full compliance is nearly impossible for any organization. For example, SOC 2 requires every employee to undergo monthly training and pass a quiz. Large organizations will never have all their employees train every single month; it’s impractical. Or consider accessing email and systems from home: unless a company operates on a zero-trust framework, which is not feasible for all, full compliance remains out of reach. Even government agencies are still using outdated systems that are far from compliant.

Before we start dictating to the private sector, we must first examine how we operate within the government. After all, the data the state holds on its citizens is just as sensitive and attractive to adversaries as the data held by private companies. While the private sector often has state-of-the-art IT infrastructure and threat detection

capabilities, governments—both state and municipal—are often running on outdated computer programs that are vulnerable to hackers. Record investment from the legislature has helped to update infrastructure and train the next generation of workers, but these investments must continue.

If we do not take these steps and approach this digital threat intelligently, we risk losing the long-term battle. Cyber threats are currently—and will continue to be if left unchecked—the greatest threat to our national security.

The time to act is now. We must adopt a proactive stance, incentivize compliance with established standards, and ensure both public and private entities are prepared for the digital battles ahead. Only then can we hope to secure our cyber future.

*Representative Mike Giallombardo is a member of the Florida House of Representatives, representing District 79. He was first elected in 2020. He chaired the Energy, Communications & Cybersecurity Subcommittee between 2022 - 2024*